

BWB:NDB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

15M 7617

-----X

UNITED STATES OF AMERICA

TO BE FILED UNDER SEAL

- against -

COMPLAINT

WILLIAM SAWICZ,

(T. 18, U.S.C. § 2252(a)(4)(B))

Defendant.

-----X

EASTERN DISTRICT OF NEW YORK, SS:

STEVEN MULLEN, being duly sworn, deposes and states that he is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

On or about and between October 2012 and July 2015, both dates being approximately and inclusive, within the Eastern District of New York, the defendant WILLIAM SAWICZ did knowingly possess one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction, the production of such visual depiction having involved the use of one or more minors engaging in sexually explicit conduct and such visual depiction was of such conduct, that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer.

(Title 18, United States Code, Section 2252(a)(4)(B)).

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with HSI for eight years. Since January 2015, I have been assigned to the Child Exploitation Group and have investigated violations of criminal law relating to the sexual exploitation of children. During my tenure with HSI, I have participated in numerous criminal investigations and, in connection with these investigations, have been responsible for the review and analysis of digital media. During my tenure with HSI, I have also assisted in investigations involving child pornography ("CP") and I have participated in the execution of search warrants and arrest warrants in connection with those CP investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous CP cases and have reviewed thousands of photographs depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

WEBSITE A

3. Since October 2012, HSI's New York Field Office Child Exploitation Group ("CEG") and Computer Forensics Unit ("CFU") have been assisting the Ontario Provincial Police ("OPP") and the Toronto Police Service ("TPS") investigate a website ("Website A") that has been used extensively by persons interested in exchanging images depicting CP. Website A has become a popular means for individuals to trade CP images and videos.

4. Website A was a file sharing website, hosted outside of the United States. Website A provided registered users with a basic "Free" access or paid "Premium" tier. Users on the basic tier were unable to access some content, and experienced slower download speeds. Website A included no search function, forums, or chats of any kind. Links were often shared on websites such as pastebin.com or via e-mail. In addition, Website A included no description, other than the file name itself, or preview of files accessible through the website. The description or preview that generated a user's interest in a particular file, therefore, would come from a referring site or an individual providing the link. Accessing Website A therefore required numerous affirmative steps by the user.

5. In approximately October 2012, OPP and TPS obtained, pursuant to a Canadian criminal code search warrant, a certain portion of Website A data, including information related to Website A usernames, email addresses, server logs, and stored content. Due to the significant volume of information seized by OPP and TPS from 32 servers leased to Website A, there was a delay in processing the information. Approximately 60,000 individuals were registered users of Website A at the time of the seizure, and the total number

of password-protected, compressed .rar ("RAR") archive files associated to those users was approximately 1.4 million. Additionally, the total size of data seized was approximately 1,500 terabytes or 1.5 petabytes. A one-terabyte hard drive will hold approximately 500,000 images or 1,000 hours of digital movies.

SAWICZ'S ACTIVITY ON WEBSITE A

6. In approximately April 2015, HSI received a subset of this information as part of the joint investigation. According to data obtained from logs on Website A, on or about August 16, 2012, an individual signed up for a "premium" account on Website A, paid \$12.99 for a 30-day subscription to the site, and registered an account using an email address. That individual registered the account on Website A and was provided with the username "5109639" and password "vi3qv7a016." That individual registered with email address "wjcs1976@gmail.com."

7. The following personal information was provided by user "5109639" at the time of the account creation: LASTNAME = Sawicz; FIRSTNAME = William; ZIPCODE = 11358; COUNTRY = United States of America; CITY = Flushing.

8. From on or about August 16, 2012 to October 15, 2012, user "5109639" utilized the "premium" account on Website A to download images that depict CP as defined by 18 U.S.C. § 2256. A review of the server log files for Website A revealed that user "5109639" was assigned IP address 24.42.68.187 during account creation and while downloading files. The log files associated with that user indicate that the user downloaded 17 RAR files. These RAR files contained over one hundred of images of CP. Open source database searches revealed the IP address 24.42.68.187 was registered to Earthlink.

9. Several of these files, which are available for the Court's review, are described as follows:

a. **SCN0708.rar contains approximately seventy-nine (79) images. One image titled "9y Hot bj.jpg"** is of a topless prepubescent girl approximately 8-10 years old with an adult male penis present in the girl's hand and mouth. It was downloaded by IP: 24.42.68.187 on 08/16/2012 at 6:50:23 a.m.

b. **SCN3107.rar contains approximately sixty-three (63) images. One image titled "10Yr Tochter 5.17 Min.jpg"** appears to be from a video and contains twenty-five frames which is of a topless prepubescent child approximately 6-8 years old with an adult male penis present in her hand and mouth. It was downloaded by IP: 24.42.68.187 on 08/16/2012 at 6:50:23 a.m.

c. **101orgnl.part1.rar (fc horewkdm3qa2).rar contains approximately three hundred and thirty-five (335) images. One image titled "P101A~1"** is of a nude prepubescent child approximately 6-8 years old performing oral sex on an adult male. It was downloaded by IP: 24.42.68.187 on 10/15/2012 at 9:33:26 p.m.

SAWICZ'S PRIOR CONVICTION FOR POSSESSION OF CHILD PORNOGRAPHY

10. In May 2008, SAWICZ was indicted in the Eastern District of New York on eighteen counts of receipt and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252(b)(1), and 2252(b)(2). On July 15, 2008, SAWICZ pleaded guilty before the Honorable Allyn R. Ross to possession of CP and knowingly downloading CP from his computer. He was sentenced to time served and 84 months of supervised release.

11. Under the terms of SAWICZ's supervised release, he must comply with all terms specified and report to the U.S. Probation Department as directed. Those terms require that SAWICZ not use a computer, internet-capable device, or similar electronic device to access pornography of any kind. Further, SAWICZ may be limited to possessing only one

personal internet-capable device to facilitate Probation in effectively monitoring his internet-related capabilities.

12. On June 26, 2015, I spoke with SAWICZ's assigned probation officer ("PO"). The PO stated that SAWICZ received authorization to possess a laptop computer (HP 15 Notebook Serial Number: CND4207HQB) to access the internet. As part of the Probation Computer and Internet Monitoring Program, monitoring software was installed on SAWICZ's laptop computer. Among other things, the monitoring software logs websites visited by SAWICZ's computer. SAWICZ's laptop is the only device he is authorized to utilize for personal purposes. SAWICZ is authorized to utilize work computers for work purposes only. The PO further stated that the only email address authorized for use by SAWICZ is an email address provided by his employer at Emblem Health care, specifically the following email address WSAWICZ76@selectemail.net.

SAWICZ'S PAYPAL ACTIVITY

13. The email address used to register on Website A by user "5109639," wjcs1976@gmail.com, is the same email address used to register two PayPal accounts; one PayPal account is registered to "Will Sawicz," and one is registered to "William Sawicz." Both accounts are registered to SAWICZ's home address in Flushing, New York (the "Flushing Address").

14. One of SAWICZ's PayPal accounts showed multiple transactions from May 2012 through February 2015. PayPal captured the user's most recent IP address as 24.199.69.230. Open source database searches revealed the IP address 24.199.69.230 is registered to Earthlink. Records obtained from Earthlink by administrative subpoena showed

that the IP address 24.199.69.230 on the date and time when SAWICZ's PayPal user logged on was subscribed to Individual A residing at 194-07 37th Avenue #1, Flushing, New York 113584004. Individual A is SAWICZ's neighbor. HSI confirmed that there is at least one unsecured network accessible from the immediate vicinity of the Flushing Address, which would include Individual A's address. Probation's computer monitoring system of SAWICZ's allowed device showed no record of activity with PayPal on the date in question. It is thus probable that SAWICZ has used and is using unauthorized computers and/or internet services, and is intentionally doing so to evade Probation's monitoring of his approved device.

SEARCHES OF SAWICZ'S HOME AND ELECTRONIC DEVICES

15. On July 23, 2015, the Honorable Steven M. Gold, Magistrate Judge, Eastern District of New York, issued a search warrant authorizing law enforcement agents to search the Flushing Address. A copy of the July 23, 2015 affidavit and search warrant are attached hereto and incorporated herein.

16. On or about July 28, 2015, law enforcement agents executed the search warrant at the Flushing Address. Law enforcement agents discovered WILLIAM SAWICZ as the sole resident of the Flushing Address. No CP was found at the Flushing Address.

17. After being told that he was not under arrest, SAWICZ told me that he purchased a Nook in 2012, and that it contains CP, including CP he downloaded in the past several months. He stated that he accesses child pornography on the Nook using google, gmail, and boyvids or boyvids 4.0. He kept the Nook at the office of his employer, locked in a right-hand desk drawer. SAWICZ provided the password to the Nook and agreed to provide the Nook to me. I accompanied SAWICZ to his office and observed him unlock the right-

hand desk drawer, and remove the Nook. He provided the Nook to me, and I provided him with a property receipt.

18. On July 28, 2015, the Honorable Vera M. Scanlon, Magistrate Judge, Eastern District of New York, issued a search warrant authorizing law enforcement agents to search the Nook. A copy of the July 28, 2015 affidavit and search warrant are attached hereto and incorporated herein.

19. On or about July 30, 2015, law enforcement agents executed the search warrant of the Nook.


20. That search revealed that the Nook contained several hundred files. An initial review indicates numerous CP images and videos. Agents reviewed a number of those files, including the following, which are available for the Court's review:

- a. **OB11_12-13.jpg** is a photo depicting a prepubescent white male sticking out his tongue while holding an adult male penis in his hand.
- b. **Fran_14.jpg** is a photo depicting a prepubescent white male with his mouth on an uncircumcised adult penis.
- c. **161609b32jmu6c8ycsccc8.jpg** is a photo depicting an approximately 50-year-old white male lying on a bed nude. Two prepubescent nude boys are with him, one on either side of the adult. One boy is seen holding the adult male's penis in his hand.

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and arrest warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target of the investigation and likely lead to the destruction and concealment of evidence, and/or flight.

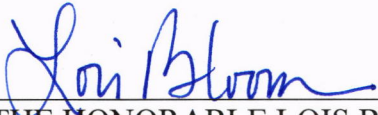
WHEREFORE, your deponent respectfully requests that the defendant
WILLIAM SAWICZ be dealt with according to law.

IT IS FURTHER REQUESTED that all papers submitted in support of this
application, including the application and arrest warrant, be sealed until further order of the
Court.



STEVEN MULLEN
Special Agent
United States Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
13th day of August, 2015



THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)194-09 37th AVENUE, APARTMENT 2,
FLUSHING, NEW YORK 11358

Case No.

15 M 0687

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 6, 2015 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:

8/23/15 3:35 pm

Judge's signature

City and state:

Brooklyn, New York

Hon. Steven M. Gold

U.S.M.J.

Printed name and title

ATTACHMENT A
Property to Be Searched

The property to be searched is 194-09 37TH AVENUE, APARTMENT 2, FLUSHING, NEW YORK 11358, further described as an attached a two-story red brick series of attached garden apartments. The PREMISES is apartment #2 located on the second floor. The outer door of the building is a brown door with two windows on the top portion of the door. These windows have a variety of American flag stickers affixed. Only apartment #1 on the first floor and apartment #2 on the second floor are accessed by this outer entry door. Two black mailboxes are on the left-hand side of this outer entry, and no names are on these mailboxes. Upon entering the outer entry door, a set of stairs with a brown handrail on the right within the vestibule lead directly up to apartment #2 on the second floor. The door to Apartment # 2 is brown.

ATTACHMENT B
Property to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;
2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:
 - a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.
7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.
11. Address books, names, lists of names and addresses of individuals believed to be minors.
12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.
13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.
14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers¹ or storage media² that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;

¹ A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

² A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
- 16. Records and things evidencing the use of the Internet Protocol addresses 24.42.68.187 and 24.199.69.230, including:
 - a. routers, modems, and network equipment used to connect computers to the Internet;
 - b. Internet Protocol addresses used by the COMPUTER;
 - c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

JAP:NDB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

15 M 0687

----- X
IN THE MATTER OF AN APPLICATION FOR A
SEARCH WARRANT FOR:

TO BE FILED UNDER SEAL

THE PREMISES KNOWN AND DESCRIBED AS 194-
09 37TH AVENUE, APARTMENT 2, FLUSHING, NEW
YORK 11358

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

----- X
EASTERN DISTRICT OF NEW YORK, SS:

KARINE STEWART, being duly sworn, deposes and states that she is a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 194-09 37TH AVENUE, APARTMENT 2, FLUSHING, NEW YORK 11358 (the "PREMISES"), further described in Attachment A to this affidavit, the items described in Attachment B to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography).

The source of your deponent's information and the grounds for her belief are as follows:¹

1. I have been a Special Agent with HSI since 2007 and am currently assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods of operations used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed thousands of photographs depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

I. DEFINITIONS

3. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

- a. The terms “minor,” “sexually explicit conduct” and “visual depiction” are defined as set forth in Title 18, United States Code, Section 2256.
- b. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . .”²
- c. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.
- d. The term “IP Address” or “Internet Protocol Address” means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0–255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other

² See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

computers have dynamic — that is, frequently changed — IP addresses.

- e. The term “Internet” refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. The term “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- g. “Chat” refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- h. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

II. BACKGROUND

4. Since October 2012, HSI's New York Field Office Child Exploitation Group ("CEG") and Computer Forensics Unit ("CFU") have been assisting the Ontario Provincial Police ("OPP") and the Toronto Police Service ("TPS") investigate a website ("Website A") that has been used extensively by persons interested in exchanging images depicting CP.

5. Website A has become a popular means for individuals to trade CP images and videos.

6. Below is a description of how Website A operated in October 2012. Website A is a file sharing website, hosted outside of the United States. Website A provided users with a basic "Free" access or paid "Premium" tier. Users on the basic tier were unable to access some content, and experienced slower download speeds. Website A included no search function, forums, or chats of any kind. Links were often shared on websites such as pastebin.com or via e-mail. In addition, Website A included no description, other than the file name itself, or preview of files accessible through the website. The description or preview that generated a user's interest in a particular file, therefore, would come from a referring site or an individual providing the link.

7. Users of the Website A file hosting service appear to have above-average technical ability, and most have taken substantial steps to obfuscate the contents of the files they upload for distribution. Many use compressed files, such as .rar ("RAR") files, that are password

protected and may contain several levels of additional password-protected, compressed archive file containers, which in turn contain large volumes of images. RAR files are data containers that store files in a compressed form. When an RAR file is extracted or uncompressed, it can contain several hundred images.

8. There are two ways to register an account, and thus become a “member” of Website A. The first requires the user provide a username, password, and email address. The second is to “quick register,” which prompts an automatically-generated username and password to be emailed to the user. Once a user becomes a member of Website A, the user will receive a registration confirmation email from Website A. Then, the user, as a member, can download or upload images and/or videos. Once a member has uploaded a file, Website A provides the user with a link that the user can share with others.

9. In approximately October 2012, OPP and TPS obtained, pursuant to a Canadian criminal code search warrant, a certain portion of Website A data, including information related to Website A usernames, email addresses, server logs, and stored content. HSI subsequently received a subset of this information as part of the joint investigation. Due to the significant volume of information seized by OPP and TPS from 32 servers leased to Website A, there was a delay in processing the information. Approximately 60,000 individuals were registered users of Website A at the time of the seizure, and the total number of RAR archive files associated to those users was approximately 1.4 million. Additionally, the total size

of data seized was approximately 1,500 terabytes or 1.5 petabytes. A one-terabyte hard drive will hold approximately 500,000 images or 1,000 hours of digital movies.

III. THE INVESTIGATION

10. On or about August 16, 2012, an individual signed up for a “premium” account on Website A, paid \$12.99 for a 30-day subscription to the site, and registered an account using an email address. That individual registered the account on Website A and was provided with the username “5109639” and password “vi3qv7a016.” That individual registered with email address “wjcs1976@gmail.com.”

11. The following personal information was provided by user “5109639” at the time of the account creation:

- 'LASTNAME' = 'Sawicz'
- 'FIRSTNAME' = 'William'
- 'ZIPCODE' = '11358'
- 'COUNTRY' = 'United States of America'
- 'CITY' = 'Flushing'

12. From on or about August 16, 2012 to October 15, 2012, user “5109639” utilized the “premium” account on Website A to download images that depict CP as defined by 18 U.S.C. § 2256. A review of the server log files for Website A revealed that user “5109639” was assigned IP address 24.42.68.187 during account creation and while downloading files. The log files associated with that user indicate that the user downloaded 17 RAR files. These RAR files contained over one hundred of images of CP.

13. Several of these files, which are available for the Court's review, are described as follows:

- A. **SCN0708.rar contains approximately seventy-nine (79) images. One image titled "9y Hot bj.jpg" is of a topless prepubescent girl approximately 8-10 years old with an adult male penis present in the girl's hand and mouth. It was downloaded by IP: 24.42.68.187 on 08/16/2012 at 6:50:23 a.m.**
- B. **SCN3107.rar contains approximately sixty-three (63) images. One image titled "10Yr Tochter 5.17 Min.jpg" appears to be from a video and contains twenty-five frames which is of a topless prepubescent child approximately 6-8 years old with an adult male penis present in her hand and mouth. It was downloaded by IP: 24.42.68.187 on 08/16/2012 at 6:50:23 a.m.**
- C. **101orgnl.part1.rar (fc horewkdm3qa2).rar contains approximately three hundred and thirty-five (335) images. One image titled "P101A-~1" is of a nude prepubescent child approximately 6-8 years old performing oral sex on an adult male. It was downloaded by IP: 24.42.68.187 on 10/15/2012 at 9:33:26 p.m.**

14. In May 2008, William Joseph Sawicz ("Sawicz") was indicted in the Eastern District of New York on eighteen counts of receipt and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252(b)(1), and 2252(b)(2). On July 15, 2008, Sawicz pleaded guilty in U.S. District Court, before Judge Ross to possession of child pornography and knowingly downloading CP from his computer. He was sentenced to time served and 84 months of supervised release.

15. Under the terms of Sawicz's supervised release, he must comply with all terms specified and report to the U.S. Probation Department as directed. Those terms require

that Sawicz not use a computer, internet-capable device, or similar electronic device to access pornography of any kind. Further, Sawicz may be limited to possessing only one personal internet-capable device to facilitate Probation in effectively monitoring his internet-related capabilities. As part of the Computer and Internet Monitoring Program, Sawicz is prohibited from sending or receiving images or videos (MMS – multimedia messaging service) via a cellular telephone as directed by the Probation Department. Sawicz is required to notify his mobile telephone provider to prevent his account from obtaining MMS on his account and to provide documentation to the Probation Department of satisfaction of this requirement.

16. On June 26, 2014, an HSI agent spoke with Sawicz's assigned probation officer ("PO"). The PO stated that Sawicz received authorization to possess a laptop computer (HP 15 Notebook Serial Number: CND4207HQB) to access the internet. As part of the Probation Computer and Internet Monitoring Program, monitoring software was installed on Sawicz's laptop computer. Among other things, the monitoring software logs websites visited by Sawicz's computer. Sawicz also received authorization to possess a T-Mobile hotspot device to access the internet. Sawicz's laptop is the only device he is authorized to utilize for personal purposes. Sawicz is authorized to utilize work computers for work purposes only:

17. Records obtained from PayPal for the email address wjcs1976@gmail.com revealed that the email address had two (2) accounts:

- a. PayPal account number 1744265705450807656 ("PAYPAL ACCOUNT 7656") is registered to Will Sawicz, was created on January 6,

2014, and uses the following address 194-09 37 Avenue, Apt 2 or Apt 2Fl, Flushing, New York 11358, United States. The account file lists a Visa debit card XXXX- XXXX - XXXX -8884, under the name Will Sawicz, Expiration Date 12/2016.

b. PayPal account number 2254719225054706497 ("PAYPAL ACCOUNT 6497") is registered to William Sawicz, was created on May 19, 2012, and uses the following address 194-09 37 Avenue, # 2, Flushing, New York 11358, and telephone number 718-309-4095. This account has approximately seven different Visa debit cards on file.

18. From on or about January 6, 2014 to March 3, 2015, a transaction log for PAYPAL ACCOUNT 7656 shows charges to the Metropolitan Tennis Group. The PO confirmed that Sawicz is a member of the Metropolitan Tennis Group.

19. From approximately on or about May 18, 2012 through February 27, 2015, a transaction log for PAYPAL ACCOUNT 6497 shows multiple transactions on this account. On February 27, 2015 at 2:41:25 PST, this account's user logged into PayPal. PayPal captured the user's most recent IP address as 24.199.69.230. Open source database searches revealed the IP address 24.199.69.230 is registered to Earthlink.

20. From on or about June 21, 2012 to July 1, 2013, the user of PAYPAL ACCOUNT 6497 logged into the account on approximately twenty (20) different dates using the same IP address, IP 24.42.68.187, that was used by Website A user 5109639 to download

seventeen (17) RAR files from on or about August 16, 2012 to October 15, 2012. Open source database searches revealed the IP address 24.42.68.187 was registered to Earthlink.

21. On June 22, 2015, Sawicz's PO made a home visit and spoke to Sawicz at his address of record: 194-09 37th Avenue, Apartment 2, Flushing, New York. According to the PO, Sawicz was allowed access to the internet for personal purposes beginning on June 19, 2014. The PO further stated the only email address authorized for use by Sawicz is an email address provided by his employer at Emblem Health care, specifically the following email address WSAWICZ76@selectemail.net.

22. Sawicz's PO stated that, based on Probation's computer monitoring system of Sawicz's allowed device, there is no record of any activity with PayPal on February 27, 2015. The PO confirmed that Sawicz has had a cellular mobile telephone with number 718-309-4035 since 2009.

23. On March 5, 2015, HSI issued a DHS Summons to T-Mobile USA requesting subscriber information for phone number 718-309-4035. On March 21, 2015, T-Mobile responded to the summons and provided the following information: the subscriber is William Sawicz, at 194-09 37th Ave., Apt. 2, Flushing, NY 11358, DOB: 9/13/1976; the account was established on October 25, 2010 and its status is "active." On March 26, 2012, T-Mobile records indicate that phone number 718-309-4035 called 866-695-2237 three times; the number 866-695-2237 was identified as ACER Computer Customer Support. As noted above, Sawicz was allowed access to the internet for personal purposes beginning on June 19, 2014.

24. Records obtained from Earthlink by administrative subpoena showed that the IP address 24.42.68.187 was outside of the retention period, and Earthlink was unable to provide the identity of the subscriber on August 12, 2012, August 16, 2012, September 4, 2012, and October 15, 2012.

25. Records obtained from Earthlink by administrative subpoena showed that the IP address 24.199.69.230 on February 27, 2015 at 02:41:25 PST was subscribed to Individual A residing at 194-07 37th Avenue #1, Flushing, New York 113584004. Individual A is Sawicz's neighbor. HSI confirmed that there is at least one unsecured network accessible from the immediate vicinity of the PREMISES, which would include Individual A's address.

26. Given the foregoing information, and based on my training and experience, I believe Sawicz, using the username "5109639" on Website A downloaded child pornography from the residence located at the PREMISES in 2012.

27. As noted above, here, on February 27, 2015, IP address as 24.199.69.230, which is subscribed to by Sawicz's neighbor, accessed Sawicz's PAYPAL ACCOUNT 6497. Probation's computer monitoring system of Sawicz's allowed device showed no record of activity with PayPal on that date. It is thus probable that Sawicz has used and is using unauthorized computers and/or internet services, and is intentionally doing so to evade Probation's monitoring of his approved device.

28. The primary purpose of Probation's monitoring of Sawicz's computers and internet access is to safeguard the community and prevent him from accessing child

pornography again. Sawicz's current evasion of that monitoring system, in conjunction with evidence that he registered and accessed child pornography on Website A means it is probably that he has again accessed and is likely compiling images and/or video of child pornography. Your Affiant submits there is probable cause, therefore, to believe evidence of violations of 18 U.S.C. Sections 2252(a)(2) and 2252(a)(4)(B) will be found at the PREMISES, to include on any computers and storage media located within the residence.

IV. THE PREMISES

29. The PREMISES is an attached a two-story red brick series of attached garden apartments. The PREMISES is apartment #2 located on the second floor. The outer door of the building is a brown door with two windows on the top portion of the door. These windows have a variety of American flag stickers affixed. Only apartment #1 on the first floor and apartment #2 on the second floor are accessed by this outer entry door. Two black mailboxes are on the left-hand side of this outer entry, and no names are on these mailboxes. Upon entering the outer entry door, a set of stairs with a brown handrail on the right within the vestibule lead directly up to apartment #2 on the second floor. The door to Apartment # 2 is brown.

V. CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

24. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child

pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

25. I know that collectors of child pornography typically retain their materials and related information for many years. In my experience, collectors of CP who use the Internet to search for and collect CP often download video and image files that they find. By downloading CP and saving it to their personal computers or attached storage devices, collectors of CP can thereby view it at any time, without having to search for it later. Even in cases where collectors of CP attempt to delete or conceal their collection of CP, forensic examinations are often able to recover CP that remains within their computers or electronic storage devices.

26. I know that some collectors of child pornography who are subject to supervision by the Probation Department try to evade the restrictions imposed on them. They do this in a number of ways, including use of unsecured internet services. As noted above, here, on February 27, 2015, IP address as 24.199.69.230, which is subscribed to by Sawicz's neighbor, was used by PAYPAL ACCOUNT 6497, which is registered to Sawicz. Probation's computer monitoring system of Sawicz's allowed device showed no record of activity with PayPal on that date. It is thus probable that Sawicz has used and is using unauthorized computers and/or internet services, and is intentionally doing so to evade Probation's monitoring of his approved device.

27. The primary purpose of Probation's monitoring of Sawicz's computers and internet access is to safeguard the community and prevent him from accessing child pornography again. Sawicz's current evasion of that monitoring system, in conjunction with evidence that he registered and accessed child pornography on Website A means it is probably that he has again accessed and is likely compiling images and/or video of child pornography.

28. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

29. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

30. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

31. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually

explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

32. I have been informed by an Assistant U.S. Attorney that the Second Circuit has noted, “[w]hen a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that ‘images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.’” United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006) (quoting United States v. Lamb, 945 F. Supp. 441, 459-60 (N.D.N.Y. 1996)). In Irving, the Second Circuit upheld a search based upon information which was more than 22 months old, noting that even though the affidavit disclosed that the defendant took care to destroy inappropriate photographs, that “there was a fair probability that child pornography would be found. . .” Id. Conversely, where there is no evidence that the subject is a collector or trader of child pornography and there is only a single incident of access to thumbnail images of child pornography on the Internet from a given Internet protocol (“IP”) address, absent any other circumstances suggesting that the suspect had accessed the images deliberately or had a continuing interest in child pornography, the Second Circuit has ruled that probable cause for a search warrant nine months later is stale. United States v. Raymonda, 780 F.3d 105, 116-17 (2d Cir. March 2, 2015). Thus, under the relevant case law, information in support of probable cause in child pornography cases is often not deemed stale, even if somewhat old, because collectors and traders of child pornography are known to store and retain their collections for extended periods of time, usually in their home

and/or on their computer. *See e.g., United States v. Allen*, 625 F.3d 830 (5th Cir. Nov. 4, 2010) (18-month delay between time period that child pornography images were accessed by defendant from peer-to-peer networking site and issuance of search warrant did not render the information stale); *United States v. Pappas*, 592 F.3d 799 (7th Cir. 2010) (officers reasonably could have relied on the search warrant that was based on child pornography sent eighteen months earlier); *United States v. Ricciardelli*, 998 F.2d 8, 12, n. 4 (1st Cir. 1993) (stating that “history teaches that collectors [of child pornography] prefer not to dispose of their dross, typically retaining obscene materials for years”); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (concluding six month old information supporting probable cause was not stale because (a) collectors of child pornography are likely to retain their sexually explicit materials; and (b) even if deleted, it is possible that the sexually explicit images could be recovered by a computer expert); *United States v. Chroback*, 289 F.3d 1043, 1046 (8th Cir. 2002) (finding three month old information sufficient to establish probable cause, when viewed in the totality of the circumstances, because collectors of child pornography tend to maintain their materials in a secure place for extended periods); *United States v. Roby*, 27 Fed. Appx. 779, 780 (9th Cir. 2001) (unpub.) (eight and one half months since the time defendant downloaded child pornography did not render the information relied on in the warrant stale); *United States v. Anderson*, 187 F.3d 649, 1999 WL 459586, at *1-2 (9th Cir. July 6, 1999) (table) (eleven month old information established probable cause where supported by expert opinion that established that child pornography collectors and pedophiles retain their contraband for long periods of

time); United States v. Sassani, 139 F.3d 895, 1998 WL 89875, at *4 (4th Cir. Mar. 4, 1998) (table) (six month old information); United States v. Lacy, 119 F.3d 742, 745-46 (9th Cir. 1997) (ten month old information in support of probable cause was not stale; affidavit stated that collectors of child pornography “rarely if ever” dispose of child pornography, and store it “for long periods” of time in a secure place, typically in their homes); United States v. Lamb, 945 F. Supp. 441, 459-60 (N.D.N.Y. 1996) (holding warrant information not stale despite five month lapse since last transmission of child pornography over internet); United States v. Bateman, 805 F. Supp. 1041, 1044 (D.N.H. 1992) (upholding warrant with seven month delay between distribution of child pornography and execution of warrant); United States v. Rakowski, 714 F. Supp. 1324, 1330 (D. Vt. 1987) (upholding warrant based on information one to six months old because “those who collect child pornography keep the pornography, do not destroy their collections, and keep the pornography accessible”); United States v. Horn, 187 F.3d 781, 786-87 (8th Cir. 1999) (“lapse of time is least important when the suspected criminal activity is continuing in nature and when the property is not likely to be destroyed or dissipated” and probable cause was not stale where the defendant had demonstrated a “deep and continuing interest in his [child pornography] collection” and it was likely that he would retain child pornography for that collection); United States v. Albert, 195 F. Supp. 2d 267, 277 (D. Mass. 2002) (concluding that, despite a four month lapse, affidavit supported a finding of probable cause where the defendant maintained a deep and continuing interest in his collection of child pornography); United States v. Shields, 2004 WL 832937, *8 (M.D.Pa. 2004) (holding that a

staleness claim was devoid of merit, where the nine month period was at issue, as “collectors of child pornography frequently possess and retain pornographic images over extended periods”); United States v. Morales-Aldahondo, 524 F.3d 115, 119 (1st Cir. 2008) (more than three years); United States v. Gourde, 440 F.3d 1065, 1071 (9th Cir. 2006)(“Having paid for multi-month access to a child pornography site, Gourde was also stuck with the near certainty that his computer would contain evidence of a crime had he received or downloaded images in violation of § 2252. Thanks to the long memory of computers, any evidence of a crime was almost certainly still on his computer, even if he had tried to delete the images. FBI computer experts, cited in the affidavit, stated that ‘even if ... graphic image files [] have been deleted ... these files can easily be restored.’ In other words, his computer would contain at least the digital footprint of the images.”) (eight months from subscription to execution of search warrant); United States v. Toups, 2007 WL 433562 (M.D. Ala. February 6, 2007) (“Further bolstering the conclusion that the staleness calculation is unique when it comes to cases of Internet child pornography is the images and videos stored on a computer are not easily eliminated from a computer's hard drive. The mere deletion of a particular file does not necessarily mean that the file cannot later be retrieved).]

IV. TECHNICAL BACKGROUND

33. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found on the

PREMISES, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

34. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on the evidence that a computer connected to a P2P network through an IP address registered at the PREMISES, there is reason to believe that there is a computer currently located on the PREMISES.

35. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic "attribution" evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file

creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

36. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for

examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.
7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.
11. Address books, names, lists of names and addresses of individuals believed to be minors.
12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.
13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.
14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers¹ or storage media² that contain records or information (hereinafter “COMPUTER”) used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;

¹ A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

² A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
- 16. Records and things evidencing the use of the Internet Protocol addresses 24.42.68.187 and 24.199.69.230, including:
 - a. routers, modems, and network equipment used to connect computers to the Internet;
 - b. Internet Protocol addresses used by the COMPUTER;
 - c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.